

Legal Studies in International,  
European and Comparative Criminal Law 7

Lorena Bachmaier Winter  
Stefano Ruggeri *Editors*

# Investigating and Preventing Crime in the Digital Era

New Safeguards, New Rights



Springer

# Legal Studies in International, European and Comparative Criminal Law


Volume 7

## Editor-in-Chief

Stefano Ruggeri, Department of Law, University of Messina, Messina, Italy

## Editorial Board Members

Chiara Amalfitano, University of Milan, Milan, Italy

Lorena Bachmaier Winter , Faculty of Law, Complutense University of Madrid, Madrid, Spain

Martin Böse, Faculty of Law, University of Bonn, Bonn, Germany

Lorenzo Mateo Bujosa Vadell, Faculty of Law, University of Salamanca, Salamanca, Spain

Eduardo Demetrio Crespo, University of Castile-La Mancha, Toledo, Spain

Giuseppe Di Chiara, Law School, University of Palermo, Palermo, Italy

Alberto Di Martino, Sant'Anna School of Advanced Studies, Pisa, Italy

Sabine Gleß, University of Basel, Basel, Switzerland

Krisztina Karsai, Department of Criminal Law, University of Szeged, Szeged, Hungary

Vincenzo Militello, Dipto Sci Giuridiche, della Società, University of Palermo, Palermo, Italy

Oreste Pollicino, Comparative Public Law, Bocconi University, Milan, Italy

Serena Quattrocchio, Department of Law, University of Piemonte Orientale, Alessandria, Italy

Tommaso Rafaraci, Department of Law, University of Catania, Catania, Italy

Arndt Sinn, Faculty of Law, University of Osnabrück, Osnabrück, Niedersachsen, Germany

Francesco Viganò, Bocconi University, Milan, Italy

Richard Vogler, Sussex Law School, University of Sussex, Brighton, UK

The main purpose of this book series is to provide sound analyses of major developments in national, EU and international law and case law, as well as insights into court practice and legislative proposals in the areas concerned. The analyses address a broad readership, such as lawyers and practitioners, while also providing guidance for courts. In terms of scope, the series encompasses four main areas, the first of which concerns international criminal law and especially international case law in relevant criminal law subjects. The second addresses international human rights law with a particular focus on the impact of international jurisprudences on national criminal law and criminal justice systems, as well as their interrelations. In turn the third area focuses on European criminal law and case law. Here, particular weight will be attached to studies on European criminal law conducted from a comparative perspective. The fourth and final area presents surveys of comparative criminal law inside and outside Europe. By combining these various aspects, the series especially highlights research aimed at proposing new legal solutions, while focusing on the new challenges of a European area based on high standards of human rights protection.

As a rule, book proposals are subject to peer review, which is carried out by two members of the editorial board in anonymous form.

Lorena Bachmaier Winter • Stefano Ruggeri  
Editors

# Investigating and Preventing Crime in the Digital Era

New Safeguards, New Rights

### *Editors*

Lorena Bachmaier Winter  
Law School  
Complutense University Madrid  
Madrid, Spain

Stefano Ruggeri  
Law Department  
Messina University  
Messina, Italy

ISSN 2524-8049

ISSN 2524-8057 (electronic)

Legal Studies in International, European and Comparative Criminal Law

ISBN 978-3-031-13951-2

ISBN 978-3-031-13952-9 (eBook)

<https://doi.org/10.1007/978-3-031-13952-9>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2022

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface: The Digital Revolution and Human Rights Challenges

Even if in the field of “technology and law,” there is always the risk that some “innovative” analysis might rapidly become outdated because of the speedy evolution of technology, we are convinced that it is worth to assume such risk and try to address the present challenges the digitalization of our lives poses for the law. Only by doing this, it will be possible to understand the future developments and, at the same time, to provide some guidance to the practitioners that have to deal with the problems originated by the use of technological devices by intelligence units, law enforcement and criminal investigators as well as criminals. And, as we all know, the legal solutions in many of these areas are lagging behind.

This is not new. It is well known that much of the technological development in the field of communications technology and the gathering and processing of data has been fostered within the field of national security and the military for preventing attacks and establishing a defensive strategy, but also to be able to counterattack war threats. And in many cases only later, when these technologies have become accessible to the citizens—*e.g.*, the use of drones or the Skype video-communication program—lawmakers have started to adjust legal frameworks to the needs and limits of the digital investigation.

This development has changed completely the way human beings communicate and behave in the present digital world, allowing to obtain a huge amount of data of every individual which provides information of almost every aspect of his or her life. In this new scenario, the challenge may lie in finding the right way to protect the right to privacy of individuals, whatever this may mean in the present world.

The aim of this book is to delve into the impact of the ICTs in the criminal prevention and investigation, by addressing the state of the art of different measures and its implementation in different legal systems vis à vis the protection of human rights. Yet this research not only pursues a diagnostic goal but furthermore aims at providing a reconstruction of this problematic area in light of modern, human rights-oriented notion of criminal justice. This broadens the scope of this investigation, which encompasses both unprecedented safeguards to traditional, or anyway widely recognized individual rights and the emergence of new rights, such as the right to

informational self-determination, and the right to information technology privacy, but also new rights as the “neuro-rights” or the “rights in the outer space.”

Moreover, although the main focus of this book is the criminal investigation, the field of security, war, and the fight of crime cannot be clearly separated, since they have not only many connecting points, but they increasingly overlap with each other when it comes to criminal activities that pose threats to the national security.

The book includes ten chapters, trying to cover the most recent developments in the area of IT and criminal prevention/investigation, overcoming the national perspectives, although referring when necessary to domestic legal rules. The list of authors has tried to combine young researchers with experience in ICTs (youth in these areas are an added-value), with senior researchers with deep knowledge in cross-border and criminal investigation/prevention field, and areas like aerospace law.

A common feature of all contributions is the providing of in-depth analysis of the multiple functions of, and consequently of the risks arising from, digital tools, in both fields of crime control and criminal investigation. Some tools prove today almost indispensable for purposes of criminal inquiries, and recourse to them often goes far beyond the limits set out by legal arrangements, and even the constitutional and international law standards. This is the case for such as trojan horses, spywares, and further malwares, which are increasingly used with a view to communication intercepts and search and seizure of digital evidence, as clearly shown by *Diego Foti* and *Viviana Di Nuzzo*, respectively. Moreover, ICTs have gained an increasing role in the area of crime prevention, and unprecedented outcomes can undoubtedly be achieved through instruments such as drones, which, as *Claudio Orlando* pointed out, do not only have enormous advantages for crime detection, but also often prove extremely useful for purposes of crime control. Further tools provide unique information with a view to avoiding criminal actions with huge impact, as *Francesca Pellegrino* highlighted by dealing with multiple potentials of satellites. All in all, the proper management of digital technology plays a key role both in ascertaining past facts with criminal law relevance and in handling new risks that are more and more linked to the cyber-realities. For both these purposes, ICTs are also of the utmost usefulness to information on spatial elements of the physical world which would otherwise be obtained with enormous difficulties. In this context, geolocation stands out as one of the most promising challenges, and the evolution of geographic information and technology has shown its great potential both in crime detection and crime prevention, as held by *Elena Militello*.

The risks arising from ICTs, notwithstanding their extraordinary utility, can however not be underestimated. While recourse to malware provides traditional means of investigation with incomparable capturing potential that magnifies the dangers of interference with the private sphere already existing in the analogical era, further digital tools highlight new risks, particularly due to the implications that can derive from an uncontrolled massive use thereof. This is the case for some surveillance techniques such as automated facial recognition, and even more, emotion facial recognition, which poses difficult problems concerning respect for a number of fundamental rights and freedoms, starting with the rights to privacy and

data protection, up to the very presumption of innocence, as widely dealt with by *Isadora Neroni Rezende*. Although such risks can surely not be justified security-based considerations, it would however be an exaggeration to affirm that ICTs endanger a human rights-oriented view of criminal justice. A very challenging task is to examine whether and to what extent digital tools can improve the standards of protection of some fundamental rights and principles by way of reducing certain inevitable shortcomings which can derive from purely human management. *Giulia Lasagni* has undertaken this task by examining pros and contras of Multi-Agent Systems in order to strengthen the efficiency and avoid some biases in the handling of criminal investigations.

Certainly, we can affirm that the outcome of this book has been a joint effort of all contributors, with cross-checks and exchange of peer reviews, which has allowed each of the contributors not only to enrich their chapters, but also to gain knowledge of realities that they were not even aware. In the scientific world, including the legal sciences—whatever this might mean—enhancing knowledge and providing new avenues for understanding reality and thus make possible to address problems, team-work is as much as necessary as in other fields of science. We can only be grateful for the willingness of the contributors to engage in this type of team-work, which has undoubtedly enriched the chapters presented in this book, but even more, has enriched the co-editors.

Therefore, we are glad to present this book to the future readers as a humble but rigorous contribution to the discussion on the need to balance the potential of technology in the criminal prevention and investigation with the protection of our privacy in this continuously changing new digital world. The next challenge to come will be perhaps how to regulate privacy and safety in the metaverse and the ways of prosecuting criminal conducts beyond the physical reality. However, this is still to come. Our aims in this book is to study the interaction of digital investigative measures and the protection of fundamental rights in the criminal prevention and investigation, but still connected to the physical reality.

Madrid, Spain  
Messina, Italy  
June 2022

Lorena Bachmaier Winter  
Stefano Ruggeri



# Contents

**Part I Crime Control and Criminal Inquiries in a Digitalised World.  
New Frontiers**

**Criminal Investigation, Technological Development, and Digital Tools:  
Where Are We Heading? . . . . . 3**  
Lorena Bachmaier Winter

**Geolocation in Crime Detection and Prevention . . . . . 19**  
Elena Militello

**Big Data and Satellites: Between Safety of Airspace and Criminal  
Liability . . . . . 43**  
Francesca Pellegrino

**Facial Recognition for Preventive Purposes: The Human Rights  
Implications of Detecting Emotions in Public Spaces . . . . . 67**  
Isadora Neroni Rezende

**Part II ICT Tools and New Investigative Techniques**

**The Use of Drones and the New Procedural Safeguards in Crime  
Control and Criminal Investigation . . . . . 101**  
Claudio Orlando

**Search and Seizure of Digital Evidence: Human Rights Concerns  
and New Safeguards . . . . . 119**  
Viviana Di Nuzzo

**Digital Privacy and Cyber-Interception of Communications . . . . . 151**  
Diego Foti

### **Part III Fact-Finding and Human Rights Challenges in the Digital Era**

<b>AI-Powered Investigations: From Data Analysis to an Automated Approach Toward Investigative Uncertainty . . . . .</b>	<b>169</b>
--	------------

Giulia Lasagni

<b>Online Hearings and the Right to Effective Defence in Digitalised Trials . . . . .</b>	<b>189</b>
---	------------

Antonella Falcone

<b>The Digital Transition in Criminal Trials: New Promises, New Risks, New Challenges . . . . .</b>	<b>213</b>
---	------------

Stefano Ruggeri

**Part I**  
**Crime Control and Criminal Inquiries**  
**in a Digitalised World. New Frontiers**

# Criminal Investigation, Technological Development, and Digital Tools: Where Are We Heading?



Lorena Bachmaier Winter

**Abstract** This introductory chapter discusses three aspects that need to be further studied to understand the impact of digitalization and new technologies in the criminal proceedings and to be able to define how criminal procedure should be structured and in which direction it should move. First, the issue of the blurring division between criminal prevention and repression caused and accelerated to a great extent due to the digital shift which claims for a new scheme on the transfer of information from the security and intelligence units to the criminal investigation authorities. Second, the fact that criminal proceedings are becoming more and more transnational, also due to the fact that the internet and the absence of territorial borders in the virtual space have consequences in the way the cross-border criminal investigation is regulated and carried out. And third, because of such ‘transnationalisation’ of the criminal activities—and criminal assets—with criminal proceedings still bound to domestic rules, it is necessary to rethink the role of criminal law in guaranteeing security in the cyberspace due to the intrinsic limitations of the current normative framework of the criminal procedure. These challenges for the future structure and role of the criminal procedure in the digital society as well as its limits in prosecuting certain cybercrimes are addressed in this chapter.

## 1 Introduction

The reader should not expect to find in these pages an in-depth or detailed doctrinal analysis—which can be found in the chapters that follow. The purpose of this introductory chapter is humbler. In addition to explaining the reasons that moved us to publish this book, it is aimed at conveying some thoughts that I consider important to bear in mind when we deal with the evolution of the criminal procedure,

---

L. Bachmaier Winter (✉)

Law Department, Complutense University, Madrid, Spain

e-mail: [L.Bachmaier@der.ucm.es](mailto:L.Bachmaier@der.ucm.es)

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022

L. Bachmaier Winter, S. Ruggeri (eds.), *Investigating and Preventing Crime in the Digital Era*, Legal Studies in International, European and Comparative Criminal Law 7, [https://doi.org/10.1007/978-3-031-13952-9\\_1](https://doi.org/10.1007/978-3-031-13952-9_1)

with a particular focus on the change of paradigm that technological progress has generated in this area of law.

The advancement of the information society has created a new context in which new challenges are to be faced in the fight against crime, for perpetrators widely use new technologies, and especially digital communication, in their illicit activities. Criminal groups and individuals, use actively digital tools and platforms for committing crimes. And at the same time, traditional crimes such as fraud, money laundering or harassment—to name just a few—have found an additional stage to expand, the virtual world or cyberspace.

This is a natural reflection of the changes that the so-called ‘digital revolution’ has produced in our societies. If people are more and more (inter)acting in the digital space, it is to be expected that criminal activities also expand in that same space, which makes it necessary to prosecute them using adequate technological instruments. The statistics of the COVID-19 pandemic confirm this appreciation; the increasing online interaction and decreasing physical movement during this time were mirrored by a higher rate of online crime and a lower rate of criminality in the physical space.<sup>1</sup>

In this scenario, however, not everything runs in favour of crime and criminals. Digital technologies also provide law enforcement agents with efficient tools to trace, detect, prevent, and investigate criminal activities. The real challenge lies in converting the drivers of the new forms of crime into new responses, within a legal framework that strikes the balance between an efficient prevention and prosecution of crime and the respect of human rights of the individuals.

In this regard, one of the main and well-known problems is the fact that the right to privacy is at risk because there is a high probability that it can be encroached by the use of preventive and investigative electronic measures, in the majority of cases without the knowledge and control of the addressee of such measures. An additional reason for concern is that, while the governments’ capacity of intrusion in our private lives has increased in an unprecedented way, the pre-conditions and safeguards for such interferences have not been clearly set out neither at a national level in many cases nor at the European level. In fact, as will be shown in the following chapters of this book, regarding the impact of the use of IT investigative tools, the access to digital data and the gathering of e-evidence in criminal investigations, not all jurisdictions have yet enacted precise legal rules on how to carry out digital investigations, which devices can be used for taking evidence, which information can be admitted as evidence at trial, which persons must be informed, and so on.

This book will highlight some of these problems with a particular focus on the impact the lack of appropriate rules and conceptual misunderstandings in the use of IT investigative tools and other digital devices might cause in the sphere of the protection of the fundamental rights in the criminal procedure. Our aim is not to

---

<sup>1</sup> See the Interpol report “Cybercrime Covid-19 Impact” of 2020, available at: <https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>.

bridge the gap between law and technology, but to clarify how some technologies are used in the criminal prevention as well as in the criminal procedure so that we can contribute to the discussion on how its use should be regulated.

There are still many other topics related to the IT tools and devices which need a further rethinking. In this introductory chapter, I will briefly draw attention to three aspects that, in my opinion, must be addressed from new and deeper perspectives to achieve a better comprehension and design of a renewed criminal procedure in the digital society. First, the dividing line between criminal prevention and repression which is increasingly being blurred, to a great extent because of the digital shift. Second, the fact that criminal proceedings are becoming more and more transnational, also due to the internet and the detachment the cloud and the communications not bound by physical borders has caused. And third, because of such “transnationalisation” of the criminal activities—and criminal assets—, it is necessary to rethink the tools which are aimed to guarantee security in the cyberspace due to the intrinsic limitations of the current normative framework of the criminal procedure.

## 2 Surveillance Versus Investigation of Crime: A New Sea Change in the Criminal Fact Finding?

The complexity of these problems is even more evident when we look at the difficulties in differentiating the borders between prevention and criminal investigation/prosecution. It is manifest that the divide between these two areas is more and more unclear. The use of big data in assessing risks, as well as the use of mass surveillance upon electronic communications, as the case *Big Brother Watch* has highlighted,<sup>2</sup> shows how much the new digital scenario has contributed to blurring the frontiers between prevention and crime prosecution. The main challenge for criminal proceedings is now to find ways to prevent that all the information, data, and potential evidentiary materials obtained under surveillance regimes flow into the criminal procedure and circumvent its procedural safeguards.

Traditionally, intelligence actions carried out by the secret services in charge of national security were kept clearly separated from the criminal investigation and outside the legal framework of the criminal procedure.<sup>3</sup> There were good reasons for that: they were considered, at least formally and legally, two separate areas that should not be mixed (*Trennungsprinzip*) and whose fields of action, although in some cases they could come close to each other, should not be confused, since their aims and methods were different. Having suffered in the past abuses of the State

---

<sup>2</sup>*Big Brother Watch and others v the United Kingdom*, Appl. nos. 58170/13, 62322/14 and 24960/15 (ECtHR, Chamber’s judgment of 13 September 2018; and Grand Chamber’s judgment of 25 May 2021).

<sup>3</sup>See Bachmaier Winter (2012), pp. 46 ff.

through its secret services, oppressing or eliminating certain groups of people (e.g., ethnic groups, religious groups, political opposers etc.), moved European countries towards a strict separation of the areas of criminal justice and secret intelligence.

However, in recent times, intelligence activities for preventive purposes have gradually acquired greater relevance in relation to certain serious criminal phenomena<sup>4</sup>—in particular terrorism, organized crime, cybercrime, and money laundering.<sup>5</sup> Certainly, intelligence has always played a crucial role in the identification, understanding and detection of serious dangers to national security and in the design of strategies to combat terrorism and other threats that might have a severe impact upon the economic, industrial and commercial interests of a country. The change comes from the fact that, at present, these intelligence units have gained more importance and occupy a leading position in the prevention and fight against certain types of crime. Their action is now considered essential.<sup>6</sup>

It has been even stated that the fight against terrorism and organized crime is unthinkable without the analysis carried out by intelligence units before an indication of criminal suspicion becomes concrete.<sup>7</sup>

More specifically, among the various factors that explain the growing role of intelligence units in the prevention and fight of serious crimes, in particular terrorism but also cyberattacks, three should be noted here.

---

<sup>4</sup>See for the German system of cooperation between intelligence and criminal investigation, e.g. Zöller (2020), pp. 79–95.

<sup>5</sup>See, for example the report of the International Commission of Jurists *Assessing Damage, Urging Action. Report of the Eminent Jurists Panel on Terrorism, Counter-Terrorism and Human Rights*, done in Geneva in 2009, p. 67, which can be accessed at <http://ejp.icj.org/IMG/EJP-Report.pdf>.

<sup>6</sup>See the “Guidelines for Starting an Analytic Unit” published by the International Association of Law Enforcement Intelligence Analysts, Inc. (IALEIA): “A lesson learned by the U.S. on September 11, 2001 was that intelligence is integral to preventing terrorist attacks. Since then, more and more U.S. Police agencies have adopted the intelligence led model, and intelligence units have been established worldwide. Intelligence led policing uses analysis in a pro-active way to effectively target criminal groups and activities. This front-end application allows agencies to assess the needs and resources of the organization and jurisdiction, placing viable alternatives in the hands of decision-makers. Strategic targeting allows the agency to prioritize cases with the highest probability of success”. On the change in the objectives of the intelligence services from the Cold War to the present moment, as well as its essential role in preventing terrorist attacks, see Trevorton (2009), pp. 15 ff.

<sup>7</sup>As it is set out in the report of the International Commission of Jurists *Assessing Damage, Urging Action*. . . , cit. in note 5, p. 67: “Intelligence plays an indispensable role in identifying, understanding, and analysing terrorist threats, in providing important hints and leads for criminal investigations and in developing effective strategies to counter terrorism. Good intelligence has always been crucial to preventing, disrupting, or subsequently punishing, criminal activity. What is new is the fact that the work of the intelligence agencies has become the most relevant acts in the panoply of counter-terrorist measures available to governments. This centrality is reflected in expanded powers of intelligence agencies, increasing international cooperation, and greater information sharing.” See also, Droste (2002), p. 117.

The first is the technological progress, which has provided intelligence units with access to multiple databases and ultimately with the capacity to process incredibly huge amount of information.<sup>8</sup>

The second is that after obtaining and processing such enormous amount of data for study and analysis purposes, as well as for preventive security aims, it has been realised that it is not only very useful for criminal detection and prosecution, but in a vast majority of cases, it is indispensable to the extent that without such data the criminal justice response could not even be activated. This explains why intelligence units have been created not only in the context of the traditional national security objectives, but also within the financial supervisory institutions—for example, for preventing money laundering and financing of terrorism—as well as at the police level. Thus, the outcome is that in practice several intelligence units deal with prevention of severe crimes, and when it comes to terrorism or cybersecurity, there will occur overlaps that require constant and effective coordination among them.

And in the third place, the increasing role that intelligence information plays in the field of criminal prosecution is also explained by the reforms implemented in substantive criminal law, as a consequence of the expansion of risk criminal offences and the criminalisation of often neutral actions at a very early stage, long before a terrorist act is actually committed.

The foregoing factors, among others, have contributed to blurring the distinction between the preventive and the repressive criminal responses, especially regarding cybersecurity, terrorism and financing of terrorism (but not only in those cases). Hence, there is a partial overlap and interrelation between the activity of the classical national security intelligence services, the financial intelligence units, the police information units, and the criminal investigation authorities, all of them being granted a vast access to data obtained by reporting obligations and surveillance.

This new scenario however does not seem to be sufficiently regulated. It is not clarified which is or should be the role of this new and expanded ‘intelligence’ in the prevention of crimes. These mechanisms are designed to detect threats and are therefore activated on unknown targets, i.e., they may affect any and every citizen even though when there is no previous suspicion against anyone in particular. This is precisely what has led to questioning the proportionality of such techniques, which intercept and store all communications with the aim of selecting which of them are worth being subjected to further analysis. There is hardly any discussion about the value that bulk interceptions can have for security operations, and about the legitimacy and reasonability of the proactive approach in identifying threats to national security.<sup>9</sup> Unlike criminal investigation, such interference in the citizens’ privacy is untargeted and operates upon selectors, without any link to a prior suspicion; which

---

<sup>8</sup>On this amount of data accessible in the information society, the growing interconnection of networks and the tendency to merge the private and public spheres of individuals, see, for example, Schermer (2008), pp. 64 ff.

<sup>9</sup>As recognized in the Report on the Democratic Oversight of Signals Intelligence Agencies, of 15 December 2015, of the Venice Commission, CDL-AD(2015)011, para. 47.



makes it understandable to question if such practices comply with the principle of proportionality, and also raises the very question of whether the test of proportionality should be different as the one applied to single criminal investigations.<sup>10</sup>

It is this regard, particular attention must be paid to studying the current caselaw of international courts of human rights (especially the European Court of Human Rights, ECtHR) and leading European constitutional courts to elucidate to what extent their caselaw provides for an adequate protection of human rights against existing mechanisms aimed at preventing risks for national security and cybersecurity, and also to what extent those courts give guidance on the impact that such surveillance measures have on our ‘digital privacy’.

Of particular interest in this context is the landmark case *Big Brother Watch* of the ECtHR,<sup>11</sup> which involves questions of compliance of the UK Regulation of Investigatory Powers Act 2000 (RIPA) with the European Convention of Human Rights (ECHR). This was not the first time that the ECtHR dealt with the question of whether intelligence regimes, and the measures that they can carry out to prevent national security risks, were in breach of the European Convention.<sup>12</sup> But this was the first time<sup>13</sup> that the ECtHR assessed the implications of digital mass surveillance mechanisms, because its previous judgments on these matters had a narrower legal or factual scope. The Chamber’s judgment on this case was delivered in 2018, and the Grand Chamber’s judgment in 2021, upholding what the Chamber had decided three years before.

The Strasbourg Court found that the rules of RIPA on bulk surveillance of telecommunications then applicable were in violation of Articles 8 and 10 of the Convention for lack of sufficient oversight of the entire selection process,

including the selections of bearer for interception, the selectors and search criteria for filtering intercepted communications and the selection of material for examination by an analysts; and secondly the absence of any real safeguards applicable to the selection of related communications data for examination.<sup>14</sup>

With respect to whether the bulk interception of communications for national security aims was legitimate and necessary in a democratic society, the Court left the assessment and balancing of the interests at stake to the national authorities,

<sup>10</sup>On the proportionality principle, see e.g. Alexy (1986), 102 Degener (1985), 43 and Emiliou (1996), 23–24.

<sup>11</sup>ECtHR judgment *Big Brother Watch and others v The United Kingdom*, of 13 September 2018, Appl. nos. 58170/13, 62322/14 and 24960/15; and ECtHR Judgment (GC) of 25 May 2021. On this judgment; see, among others, Bachmaier Winter (2021), pp. 17 ff.

<sup>12</sup>See the ECtHR, *Weber and Saravia v. Germany*, judgment of 29 June 2006, Appl. no. 54934/00; *Liberty and others v the United Kingdom* Appl. no. 58243/00, of 1 July 2008; *Roman Zakharov v Russia* Appl. no. 47143/06 (GC), of 4 December 2015; *Szabó and Vissy v Hungary* Appl. no. 37138/14, of 12 January 2016; *Centrum för Rättvisa v Sweden* Appl. no. 35252/08, of 19 June 2018.

<sup>13</sup>In addition to *Centrum för Rättvisa*, a case which also dealt with a digital mass surveillance regime.

<sup>14</sup>*Id.* (Chamber), para. 387.

which “enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security”. Nevertheless, the Court explicitly recognized that the reports provided by the British independent reviewer on terrorism legislation and by the Venice Commission show that the operation of a bulk interception regime to discover unknown or unidentified targets “is a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime”.<sup>15</sup> The Court confirmed that the decision to operate a bulk interception regime to identify unknown targets falls within the State’s margin of appreciation.<sup>16</sup>

The ECtHR also concluded that, as the risks of secret surveillance increased so much in the “technological sea change”, the safeguards provided in its previous case law assessing strategic surveillance measures (mainly in the cases *Klass* and *Weber and Saravia*) can no longer be considered sufficient. Questions as whether a “prior independent control by a judicial authority should not be a necessary requirement in the system of safeguards” were raised in the dissenting opinions.<sup>17</sup>

Bulk surveillance is thus considered legitimate for national security purposes, and the necessity test is linked to the oversight mechanism. Proportionality is left to the margin of appreciation of the States.

Taking a closer look at the differences between criminal procedure and intelligence regimes, the main difference is that, unlike in the former, in the latter the utility test (how useful this mechanism is for detecting threats for national security) and the necessity test (whether there is a less restrictive measure to achieve the same results) can as a rule not be checked with regard to individual cases, but only on the basis of the data reflected in the internal auditing reports and those prepared by the independent commissioner. The *ex post* control by an independent commissioner shall fulfil this task, although it naturally will not cover all files or records.

The ECtHR was completely aware of this difference. Therefore, it held that the impossibility to determine whether the same preventive aim could have been achieved by other less intrusive means than the bulk interception of communications made it necessary to rely on the assessment made by national lawmakers and on the reports produced by the independent oversight bodies.

The two most distinctive elements in relation to safeguards in the criminal investigation are the requirements of the previous suspicion and the *ex ante* judicial warrant. In the interception of communications within a criminal investigation, the initial control requires a grounded judicial warrant, checking the lawfulness and all the elements of proportionality, considering the existence of a suspicion against an individual. The targeted interception for criminal investigative purposes is subject to

---

<sup>15</sup>Id., para. 386.

<sup>16</sup>Id., para. 314.

<sup>17</sup>See *ibid.*, partly concurring, partly dissenting opinion of Judge Koskelo, joined by Judge Turković, para. 20. The possibility for such a prior mechanism of prior judicial or independent authorisation is illustrated by the Swedish legislation, as seen in the *Centrum för Rättvisa* cited above.

control at all stages by the judicial authority and, in addition, the *ex post* control will be open to the defendant as well as to the adjudicating court.

Of course, the approach in the case of non-targeted surveillance differs completely from the one adopted on targeted interceptions. There is no initial decision based on a previous suspicion simply because there is no target. This is logical once the assessments on suitability and necessity of the measures are accepted. The minimum necessary indications, or the suspicions, that must be present in a criminal case in order to allow a targeted interception of communication are not applicable to the situation of unknown targets being subjected to bulk interceptions.<sup>18</sup>

All these differences call for a ban on allowing the intelligence information to flow without restrictions into the criminal proceedings. However, in practice, this exchange might not be kept under control, precisely in those areas where the intelligence unit is authorized to carry out surveillance measures in the area of prevention of serious crime and terrorism.

### 3 Digital, Global, and Transnational: Some Notes

The digitalisation has also caused an unprecedented increase of the ‘transnationalisation’ of the criminal proceedings as well as a ‘delocalisation’ of evidence, a reality that also requires a new legal approach to overcome the traditional national view of investigative measures.

Regarding the investigation of cybercrime—as well as other types of cross-border crimes—and the impact of the digital data and e-evidence on criminal investigations, very few systems establish rules on how to obtain the digital evidence located abroad or in the cloud.<sup>19</sup> In many cases, there are no rules at a national level about how to carry out computer searches in order to keep them within the proportionality requirements, and also to prevent disclosing confidential information (as for example, lawyer-client privileges).<sup>20</sup> And even when these national rules exist, they offer significant differences between them, and thus the absence of harmonisation can prevent the admissibility of the evidence obtained through online cross-border measures.<sup>21</sup>

Indeed, despite the rules introduced by the CoE Convention on Cybercrime,<sup>22</sup> the legal provisions on access to digital data and ensuring its integrity are still

<sup>18</sup> See *Big Brother Watch* (Chamber), para. 317.

<sup>19</sup> For a comparative study at the European Union level see Sieber and Von zur Mühlen (2016). See also Bachmaier Winter (2017), p. 3 ff.; Soares Pereira (2019), p. 248 ff.

<sup>20</sup> On the lawyer-client privilege in a comparative view, see Bachmaier Winter and Thaman (2020), pp. 37 ff.

<sup>21</sup> Bachmaier Winter (2017), pp. 317 ff.

<sup>22</sup> CETS 185, of 23 November 2001.

fragmented at a national level, something which is causing problems for its access and transfer, and also with regard to the admissibility of e-evidence. This is the reason that led to negotiating at the Council of Europe level an adequate legal framework to overcome those obstacles in accessing and using electronic evidence. After almost four years of intense negotiations, finally on the 17 November 2021 the Committee of Ministers of the Council of Europe adopted the Second Additional Protocol to the Budapest Convention on Cybercrime.<sup>23</sup> It is still to be seen to what extent the present problems on accessing electronic evidence will be overcome in the future. For the moment the Second Protocol is open for signature by the CoE member States, and the EU Council has authorised the EU member States to sign it.<sup>24</sup>

Furthermore, in the fields in which the cross-border evidence plays an increasingly important role, it is no longer sufficient to provide for the protection of procedural safeguards at a national level, because the data and the communications electronically stored may be used in a different jurisdiction than that in which those communications took place. The recent developments by the European Commission on the e-evidence Digital Exchange System (e-EDS)—an initiative which is part of the broader Digital Criminal Justice project<sup>25</sup>—includes the establishment of a single electronic platform to exchange the most frequently applied instruments for judicial cooperation. This will enable a reliable transfer of electronic evidence with a view to ensuring its authenticity and integrity. Once such a secure exchange platform is operating, the transfer of e-evidence among the EU Member States will be facilitated, and the checks and safeguards for the integrity and authenticity of the e-evidence will be strengthened. However, the access, the admissibility, and the assessment of the evidence obtained abroad will still be a challenge. Common rules and principles are still to be developed, to guarantee that the protection of human rights will not be lowered by facilitating the transfer of evidence across States.

---

<sup>23</sup>Second Additional Protocol to the Budapest Convention on enhanced cooperation and disclosure of electronic evidence, adopted on 17 November 2021, and opened for signature on 12 May 2022. The rules included in this Protocol aim at providing tools for enhanced co-operation and disclosure of electronic evidence—such as direct cooperation with service providers and registrars, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies or joint investigations—respecting human rights and rule of law, including data protection rights.

<sup>24</sup>Council Decision (EU) 2022/722, of 5 April 2022 authorizing Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, O.J. of 11.5.2022, L/134/15.

<sup>25</sup>See the Communication from the Commission “Digitalisation of justice in the European Union. A toolbox of opportunities”, Brussels, 2.12.2020, COM(2020) 710 final, accessible at <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:710:FIN>.

## 4 Cybercrime *Versus* Cybersecurity: Criminal Investigation or Resilience?

The digital society poses new challenges for the security of individuals, above all from the points of view of resilience against cyberattacks, preventing crime, and protecting human rights. Cybersecurity is a major concern in our societies, and some figures may illustrate the magnitude of the problem. According to some projections, costs of data breaches will reach \$5 trillion annually by 2024, up from \$3 trillion in 2015.<sup>26</sup> A recent survey of the EU showed that most people in the EU (55%) are concerned about their data being unlawfully accessed. According to the European Union Agency for Cybersecurity (ENISA) report for 2018,<sup>27</sup> a total of 351,913,075 unique malicious URLs were identified, representing an increase in the number of malicious URLs compared to previous year totalling 282,807,433. Child pornography exchange has increased a 500% during the pandemic.

The European Union Security Strategy, published on 24 July 2020,<sup>28</sup> confirmed that cyber-attacks and cybercrime continue to rise, and security threats are also becoming more complex. They feed on the ability to work cross-border and on inter-connectivity, and they exploit the blurring of the boundaries between the physical and digital worlds; they tend to exploit vulnerable groups, social and economic divergences.<sup>29</sup>

According to the EU institutions, all these areas are to be addressed under one main principle or concept: resilience.<sup>30</sup> Of course, in achieving this specific aspect of resilience, technical, scientific, social, and political layers are to be interlinked. All these aspects need an adequate legal framework and, according to the ENISA Report Conclusions,

several barriers do exist in Europe and worldwide that hinder access to CTI information, such as the existence of diversified regulatory spaces, the unavailability of reliable incident information and deficiencies in information sharing.

A priority in this context is to study the interactions of cybersecurity, and the connected concept of resilience, and to examine the prosecution of cybercrime and cyberattacks. Regarding cybersecurity, it is necessary to address how the concept of

---

<sup>26</sup>Juniper Research, *The Future of Cybercrime & Security* (2018), p. 4 ff., accessible at <https://www.sciencedirect.com/journal/computer-fraud-and-security>.

<sup>27</sup>Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

<sup>28</sup>COM(2020) 605 final.

<sup>29</sup>The main areas to be addressed according to the EU strategy are: Cybercrime, the Networks and Information Security (NIS), the EU Defence Agency (EDA), Cyberdefence, in the intergovernmental pillar of the EU.

<sup>30</sup>In this realm, resilience is defined as “the ability to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation” (ENISA 2011).

resilience can be implemented in all linked areas, as for example through providing a better legal framework, establishing a supranational institutional investigation and prosecution authority, and increasing the public-private partnership to facilitate technical assistance. There is also a need to analyse which impact these actions adopted within the context of cybersecurity by public and/or private entities will have on the criminal investigation of cybercrimes, and how they will share valuable information and evidence for criminal prosecution purposes with law enforcement.

It needs to be further explored what the role of the criminal investigation and prosecution is in the field of cybersecurity, since the objectives of the criminal law and criminal prosecution are not precisely aiming at resilience, but through an effective sanctioning system provide deterrence in the committing of criminal conducts and also give guidance on what are the most precious values of a specific legal order in a certain time. Such aims might function in certain areas but are hardly effective when facing cyberattacks not linked to a concrete territorial jurisdiction or person. The study of the existing barriers is also significant in the criminal justice response, precisely considering that cybercrime is in essence a cross-border crime and evidence might not be easily accessed, which might open the door to use the concept of procedural resilience, as many criminal investigations on cyberattacks/cybercrimes will hardly lead to the identification of cyber-offenders or to their prosecution and sanction. All this should make us reflect on the application of the principle of mandatory prosecution, as it will be pointless to open a criminal investigation where it is already foreseeable that the perpetrators will never be identified and, if identified, there is hardly any chance that they will be brought to justice. Finally, there is also an element that needs to be recast within the criminal procedure in fighting cybercrime, which is clearly linked to the actors that provide cybersecurity: the role of public-private cooperation regarding cybersecurity and fighting cybercrime, and the risks that such partnerships may entail.

In these areas, the main current challenge is likely to determine whether the same standards and tools can be deployed in cybersecurity and the prevention of cybercrime, and to which extent it is possible to share information on cyberattacks among States for the purposes of criminal investigation. While a security policy against foreign cyberattacks may stick to the concept of resilience, so that the conflict is not escalated with public attribution and retaliation against the foreign attacker, in the criminal law realm the response should go beyond the resilience territory and reach the prosecution and sanction. The differences in addressing cybersecurity threats in the foreign policy and in criminal law, and when the two areas may converge, must be analysed from a “holistic” or interdisciplinary point of view; criminal proceedings cannot be instituted without taking into account the security policy and the cybersecurity elements.

It goes without saying that the first step to achieve some coherence in the criminal prosecution of cybercrime is to raise awareness of the challenges for security in the present digital society, be conscious that there are overlapping fields of cyberattacks, cyberwar and cybercrime, all encompassed under the broad concept of cybersecurity, and that the boundaries of international law, security and prevention of crime and prosecution and sanctioning of criminal conducts has become less clear.

While at the level of international security we must face the question of how much evidence it is necessary to produce to attribute publicly a cyberattack to another country, at the level of cybercrime it will often be more and more necessary to count with the support of private companies to identify the perpetrator. The various instruments to prevent cyberattacks and to react against them will inevitably be overlapping and even conflicting at times. All these factors require a new approach in the criminal proceedings during the investigation of certain types of cybercrime, where the concept of resilience may also become relevant.

## 5 Final Remarks

A constant feature in history is that human beings have used and developed technical instruments to face immediate needs. As scientific knowledge advanced, technology also became more and more sophisticated (sometimes raising new needs in mankind), but typically humans were in command of technology and decided its course of action. This might be changing with self-learning machines, which will be capable to take decisions in an independent fashion. The law cannot stay behind technological evolution. And the protection of human rights, which is a especially significant part of the law, must advance at the same pace as the technology if we want the IT society to respect the rule of law and comply with human rights conventions and the essential national and supranational constitutional principles in this realm.

This applies especially to criminal proceedings, where the State can use powerful means against individuals, and even more in a world where AI allows processing data in a measure, and at a speed, that were unimaginable some decades ago. The ever-growing tempo of scientific and technological development, and the immense possibilities that AI offers, cannot but affect the content of this book. Some of the issues that are treated here as novel may perhaps become in a few years matter for the study of the history of criminal procedure.

Even if some of the technological instruments studied in the chapters of this book may become soon outdated, the big challenge of finding a balance between the aim of criminal procedure and the protection of fundamental rights will always be present. The need to become aware of the reach of IT investigative measures in the sphere of privacy—a notion that is very different from the traditional concept of privacy that emerged from the bourgeois pre-industrial society—is today more important than ever. In the era of the IT society, the debate about the principles of necessity and proportionality as criteria to justify and limit interferences with fundamental rights has acquired even more relevance.

This may also be an opportunity to rethink the classical structure and goals of the criminal procedure, in a context where a large amount of evidence is generated without direct connection with the commission of a crime and therefore pre-date the criminal proceedings. This is not a novelty in itself, for many evidentiary sources exist prior to the initiation of a criminal proceedings, and the criminal investigation is aimed precisely at discovering them. After all, something similar occurs in civil